

IDS and Penetration Testing Lab

ISA656

(Attacker)

Ethics Statement

Network Security Student Certification and Agreement

I, _____, hereby certify that I read the following:

University Policy Number 1301: Responsible Use of Computing

<http://www.gmu.edu/facstaff/policy/newpolicy/1301gen.html>

I understand that GMU takes its ethical obligations very seriously and violations will not be tolerated. I fully understand that GMU and its students must conduct the Program's activities in accordance with the highest possible ethical and legal standards. I know that I am responsible for ensuring that my personal conduct is above reproach. As a condition of studying in the ISA Program at GMU, I agree that violations of the standards described in the Code of Conduct shall be made known immediately to my appropriate faculty member(s) and that violations will result in dismissal from the Program and failure to receive the degree. I understand that this is a zero tolerance policy and that no second chances are given.

I agree to take all reasonable precautions to assure that sensitive University or faculty information, or information that has been entrusted to my fellow students or me by third parties (such as the students' employers), will not be disclosed to unauthorized persons. I understand that I am not authorized to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the faculty or the person who is the designated information owner or custodian.

I also understand specifically that GMU provides computer systems and networks for my use in academic studies and that I am not permitted to use those computer systems and networks for personal business or for any activities not related to my academic studies. I understand that GMU audits and monitors the use of those computer systems and networks and that I have no right to privacy or expectation of privacy when I use computer systems and networks provided to me by GMU.

Signature

Printed Name

Purpose:

This lab will expose you to various techniques and tools including protocol analyzers, network scanners, Intrusion Detection Systems, and Penetration tools. Attackers, whether hackers or penetration testers (or ethical hackers), follow certain techniques and steps when trying to hack into their target systems. We will explore these techniques and perform hands on exercises to illustrate these techniques and give you a better understanding of attacking as well as defending methodologies.

Techniques:

When trying to attack their target systems, attackers usually go through the first phase of reconnaissance. In this phase, attackers try to map out the network they are trying to attack and understand the architecture of the network. The next step usually involves scanning targets for vulnerabilities. These scans could be noisy and could trigger alerts on a target network especially when it has monitoring devices like an Intrusion Detection System. Another type of scanning is passive scanning, a silent scan based on traffic it detects and sees from the network, without having to send any packets to the target. Once some vulnerability is discovered, attackers usually use existing exploits or if more advanced, write exploit codes for certain vulnerabilities. The next step would be to launch an attack to exploit the vulnerability and try to gain access. Finally, attackers would do some cleaning of their traces and try to maintaining access to the system by installing root kits and backdoors.

Software Requirements:

1. VMware workstation.
2. Network Security Toolkit appliance (NST v.1.5.0). (Includes Snort IDS, Wireshark protocol analyzer, Nmap scanner, Nessus scanner, and other useful security tools)
3. Backtrack3 Beta, penetration testing appliance.

Lab Exercise:

1. Download the Network Security Toolkit (NST) appliance from the following link:

http://sourceforge.net/project/downloading.php?groupname=nst&filename=nst-vm-1.5.0.zip&use_mirror=internap

2. Locate your NST appliance. (nst-vm-windows-1.5.0.vmx file under "nst-vm-1.5.0" folder)
3. Before starting the virtual machine, verify that the network connection type for Ethernet devices is "bridged". Also you can increase the memory device to around 500 MB.
4. Start the image and login using:

Username: root

Password: nst2003

5. You can close the browser and Start a terminal. Identify the IP address of your guest machine (Right click on the desktop and under "desktop applications" choose "Aterm Terminal" to get a terminal).
6. Identify your host and guest IP addresses for you and get the same information for your partner. Fill out the following table:

| IP information | host (windows) | guest (Linux) |
|----------------|----------------|---------------|
| You: | | |
| Your partner: | | |

7. At this point, you are ready launch attack1. This involves using Nmap scanner to scan your partner's computer and find out what open ports the partner has. Keep in mind that this is the reconnaissance phase to identify services that the target could be running. On your terminal (guest machine) cd to /usr/local/bin/. Type the command for performing a TCP Null scan (no flags set) on the target computer. Your target is your partner's host computer. Before you run the scan, notify your partner. If the command is done, launch the same command again to continue scanning. At this point,

you could be performing a Denial of Service if you can saturate the target with these scans.

Which command did you use? _____.

(Answer) `nmap -sN (target IP)`

Note: Do not provide command information to your partner as it is the partner's job to perform packet analysis and find out what type of scan you have performed.

8. Now we need to launch attack2. This time we will use the Nessus security scanner. To run Nessus, on your guest machine, open up a terminal and add a Nessus user by issuing the following commands:

```
Cd /etc/nessus
```

```
Nessus-adduser
```

9. Choose a login username. Use pass (password) for authentication, and type the password twice. Use Ctrl + D to finish and hit ok.

10. Now you need to install Nessus plugins. Each plugin checks for a specific vulnerability. Nessus currently has around 21000 plugins. A group of plugins is already downloaded. Perform the following commands to unzip/decompress the downloaded file.

```
Cd /usr/local/lib/nessus/plugins/
```

```
Tar -xjf nessus_plugins.tar.bz2 -C /usr/local/lib/nessus/
```

```
ls | wc -l
```

(The last command displays the number of files in the current directory. You should see around 1124)

11. Now we need to update plugins to make sure we are using the latest attacks. Perform the following steps:

- a. Try the following command:

```
/usr/local/bin/nessus-fetch --register 96B1-C361-ACD0-DA87-CBC2
```

(If the activation code works, plugins are updated and you are done. If not then you can get your own activation code for free, see steps below)

- b. Go to

<http://www.nessus.org/plugins/index.php?view=register>

- c. Complete registration and get the activation code

d. Repeat the command in 'a' with the new activation code as in:

```
/usr/local/bin/nessus-fetch --register (NEW ACTIVATION CODE)
```

12. Once plugins are updated and you have a Nessus user, you need to run the Nessus Daemon by issuing the following command:

```
/usr/local/sbin/start_nessusd
```

```
Ps -eaf | grep nessusd
```

(Last command to verify that the daemon is running; you should see nessusd with process ID listed)

13. Type the following command to start the Nessus client:

```
/usr/local/bin/nessus
```

You should leave "localhost" as the Nessusd Host and '1241' as the port. Use the login name and password you created when you added the Nessus user, and hit "login" button. (Might prompt you to accept certificate, please accept the cert).

14. Under the plugins tab, you can choose "enable all".

15. Under the target tab, type in the IP address of your partner's guest machine.

16. Verify with your partner that he is ready before you hit the "start scan" button to launch attack2.

17. When scan is done, you should see the Nessus report. Click on the target's host IP address, and identify ports and possibly vulnerabilities and severities. Provide one of these vulnerabilities:

12. Notice again the phases of attack. After performing the reconnaissance, you are now identifying possible exploits. Next you could write (or use) some tools to exploit these

vulnerabilities. The following is an open attack session where both you and your partner will try to attack each other's machines.

13. Now we are ready for the second part of this lab. This time you will have the freedom of trying to attack your partner's host computer. Your partner will also be doing the same. If you truly manage to hack your partner's computer, you will get extra credit on this lab. After finishing this part, you will realize how harder it is to attack than it is to defend. The lab will provide you a famous penetration testing VMware appliance that already has many hacking tools. It's called Backtrack, and we will be using the latest beta version 3. Please go ahead and shutdown your current VMware machine. Follow the following steps to get your attacking system ready.
 - a. Download the Backtrack 3 ISO file, called "bt3b141207" to your Windows XP Host machine from the "IDS_LAB" folder.
 - b. In VMware click on the **File** menu and select **New Virtual Machine..**
 - c. Click the **Next** button
 - d. Select the **Custom** radio button, click the **Next** button
 - e. Select the **Linux** radio button, select **Other Linux** in the Version drop-down box, and click the **Next** button
 - f. Type **Backtrack** in the Virtual Machine textbox and click the **Next** button
 - g. Click the **Next** button again.
 - h. Accept the default for the Network Type and click the **Next** button.
 - i. Accept the default for the I/O adapter type and click the **Next** button.
 - j. Accept the default for the Disk and click the **Next** button.
 - k. Accept the default for the Disk Type and click the **Next** button.
 - l. Accept the default for the Disk Capacity and click the **Next** button.
 - m. Type **Backtrack.vmdk** in the Disk File textbox and click the **Finish** button.
 - n. Edit the virtual machine settings for the Backtrack virtual machine.
 - o. Highlight the Hard Disk device and click the **Remove** button.

- p. Highlight the CD-ROM device and select the **Use ISO image:** radio button.
 - q. Click on the browse button and point it to the "bt3b141207" file that you downloaded to your Windows XP Host machine.
 - r. Click on the **OK** button.
 - s. Click the **Start this virtual machine.** Your Backtrack should be up and running.
14. Now you are free to play around with this appliance and use the tools to attack your partner. Keep the following points in mind:
- a. Do NOT attempt to attack other than your partner's host computer.
 - b. Do not unplug your network cable to avoid attack from your partner!
 - c. Try to go to the start menu and under the Backtrack menu, you should see a list of tools categorized by the phases of attacks we talked about earlier.
 - d. As a hint, try to first scan your partner's computer and try to identify the type of ports that are open. Then try to find vulnerabilities associated to these open ports. For example if they have a web server with port 80 open, try to identify the version of that web server and look for vulnerabilities. The next step would be to try to launch attacks. Backtrack3 has an exploiting framework called Metasploit. It has a good list of exploits that could be used against your partner's computer. Try to learn how to launch them. The web interface is easier to use (try Framework3-Msfweb. After running that daemon, open up your browser and type:

<http://127.0.0.1:55555>

You should see the Metasploit framework. Based on your reconnaissance attempts, try to choose the corresponding exploits and launch them against your partner.
 - e. Write down which exploits you tried and if any worked for you:

References :

1. <http://www.snort.org>
2. <http://base.secureideas.net/>
3. <http://www.nessus.org/plugins/index.php>
4. <http://www.vmware.com/appliances/directory/141>
5. <http://www.wireshark.org/>
6. Snort 2.1 Intrusion Detection by Baker, Beale, Caswell, and Poore.
7. <http://www.ethicalhacker.net/>
8. [http://backtrack.offensive-security.com/index.php/Main Page](http://backtrack.offensive-security.com/index.php/Main_Page)
9. www.remote-exploit.org/backtrack.html